
1Manjuprasad B, 2Andhe Dharani
1Research Scholar, 2Associate Professor
Department of MCA, R.V College of Engineering, Bangalore, India

ABSTRACT

Wireless Sensor network is a recent advance trend in wireless communication and has a vast application in various filed. In this view WSNs need an efficient mechanism for routing or transmitting data, simple computational process and optimal energy usage and last but not the least the security. Currently many existing research works aiming to achieve the WSNs objectives but its needed to be updated as a technology grows, for example energy is not an issues for terrestrial WSNs as many latest technology are adopted by sensors so that it can harvest the energy from the environment itself. Like this security is also not an issue in some of the application of sensor networks. This a survey on security issues in WSNs, as many survey on security just glanced on the different security issues, challenges, solution but this paper aims to unearth the need of security in WSNs based on the types of applications for which the nodes are deployed.

Keywords: Wireless Sensor Network, Sensor Nodes, Message Authentication Code, Jamming, Tampering.

1. INTRODUCTION

A wireless sensor network (WSN) is an assortment of numerous tiny nodes called as sensors that are connected with a petite range of some wireless links or channels like 802.11, 802.15.4[1]. This links are able to connect these nodes to some infrastructure to forward the collected or aggregated information to the centralized base station. Sensor nodes are equipped with low resources like battery, memory and with a low complex processing ability[2]. These WSNs is a network of infrastructure composed of sensing, computing and communication elements that enable administrators to observe and react to events and phenomena in a specified environment or applications [3].

The most recent trends in WSNs are the hard core of internet of things (IoT), and it is a blistering topic in the current research field [4]. Due to these characteristics WSNs has a very wide range of applications mainly divided into two categories: Monitoring and tracking in many fields such as real-time traffic analysis, habitat monitoring, and battle field reconnaissance. In all of these cases, a group of sensor nodes works in a monitored area, senses data from the field, and sends data back to a base station, where the data analysis takes place. The most important purpose of sensor networks is to answer queries about the status of the monitored area, such as calculating tracks of monitored objects, temperature, or enemy activity. In the transition to next-generation computing devices, the importance of WSN are self-evident. Therefore, more and more attentions have been paid to the development of WSN by the academia and industry [5] [6]. Wireless sensor networks must be considered how to add security mechanisms to protect the sensor nodes to communicate securely. Many such mechanisms have been designed according to the characteristics of the
wireless sensor network. Due to the resource constraints it is difficult to directly employ the conventional security mechanisms in WSNs, so there is a necessary to understand the limitations in this area [7][8].

The rest of the paper is organized as follows: Section 2 presents the need of security and requirements to achieve security in WSNs. Section 3 scripts the challenges and issues in securing WSNs.

II. SECURITY ON WIRELESS SENSOR NETWORKS

Security is the one of the important issue in all fields and it not limit to wireless sensor network [9]. But it is considered as complex problem in WSNs due to the medium and the devices constraints [10]. Thus, many security protocols were proposed trying to efficiently carry out the problem of security and the constraints of wireless networks [11, 6, 12].

Need of Security

When coming to security the first question arises is why there is a need of security in WSNs or any other communication networks or anywhere [13]. This is to protect the physical or logical asset or information from unauthorized person or system, accidently or intentionally.

Security in WSNs

- In many application the data obtained by the sensing nodes need to be kept confidential and has to be authenticated.
- Without security a malicious node could intercept private information or sometimes could send false messages to the other nodes in the networks.

Even though there is no need of security in the application of habitat monitoring and tracking applications[14,15], but security play an important role in battle field surveillance where security is very essential. Security depends on the purpose of the specific application for example sensors deployed for just recording the temperature for weather forecasting application is different from sensors deployed for detection of forest fire. In weather forecasting the security may be compromised but in the forest fire it can’t because if some people try to destroy the forest resources by modifying the sensor deployed to monitor, if there is no secure system so these can lead to loss of natural resources, like this many application need a secure system for efficient information transmission with efficient resource utilization of WSNs.

Security in WSNs can be afford by the following requirements

Security services should be Confidentiality, Integrity, Authentication and Freshness [16, 17].

Confidentiality: The data that is processed by the sensor nodes which is to be sent to other trusted nodes must be kept in secret from any unauthorized entities in the network. This is one of the complex issues in WSNs because of the broadcast nature of the sensor nodes, so the security protocol applied for unicast communication cannot be applied or suitable for WSNs.
The standard approach for confidentiality is to encrypt the data with a secret key that should be able to use only by the authorized personal. But cryptography is too expensive to apply for the resource constrained sensor nodes.

**Integrity:** Integrity means that the message that is being communicated by the trusted nodes should be un-altered during the transmission from a source to destination node by any malicious node. This is usually done in conventional network using MAC (Message Authentication Code) or digital signatures.

**Authentication:** Is the process of identification that the receiving nodes are sure that the message it receives comes from a legal source and the sending nodes ensure that the message is received only by the authorized nodes [18].

**Data Freshness:** If a node sends a message to some destination it should ensure that there is a minimum delay, but while transmitting some intermediate or malicious nodes may try to hold the data for a sometime so that the data sent will be waste when it arrives at the receiving nodes. This plays a vital role in some application where the information should be communicated in time. So security is vital aspect in WSN applications [7, 19].It is important therefore to consider security solutions that guarantee data confidentiality, authenticity, integrity and freshness.

### III. SECURITY CHALLENGES IN WIRELESS SENSOR NETWORKS

The reason why it is a complex task while providing a security for wireless sensor networks is because of the various types of attack that make a security protocol complex. The Attacks on wireless network can be broadly divided into 3 main classes [20, 21] as shown below:

**Interception** is an attack on confidentiality, the sensor nodes may be compromised by an opponent node to gain unauthorized access to sensor node.

**Modification** is an attack on integrity. Modification means an unauthorized node not only accesses the data but tampers it, for example by modifying the data packets being transmitted.

**Fabrication** is an attack on authentication. An adversary node injects false data and tries to compromises to share the information transmitted.

To implement a security protocol to WSNs one should know what are the types of attack that can compromises the security and decrease the performance of WSNs. So the attacks can be classified according to each layer of the WSNs OSI model [20, 21, 22] which as shown in the below figure

<table>
<thead>
<tr>
<th>OSI Layer</th>
<th>Types of Attack</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical layer</td>
<td>Jamming, Tampering</td>
</tr>
<tr>
<td>Data link layer</td>
<td>Collision, Eavesdropping, Resource exhaustion, Traffic analysis</td>
</tr>
<tr>
<td>Network layer</td>
<td>Spoofing, black hole/ Sink holes, Sybil attacks, Denial-of-service (DoS), Wormholes Flooding, Hello Flood Attack</td>
</tr>
<tr>
<td>Transport layer</td>
<td>Injects false messages, Energy drain attacks</td>
</tr>
<tr>
<td>Application layer</td>
<td>False data injections, Attacks on reliability</td>
</tr>
</tbody>
</table>
In fig- we can observe the types of attack that can affect the performance of WSNs. Now these attacks can be analyzed so that in what ways they are harmful to WSNs. Table below parameters of WSNs which is more affected due to specific attacks.

<table>
<thead>
<tr>
<th>Types of Attacks</th>
<th>Resources Wastage</th>
<th>Decrease in Performance</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Energy</td>
<td>Bandwidth/Channel</td>
</tr>
<tr>
<td>Jamming, Tampering</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Collision</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Eavesdropping</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>DoS</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Hello Flood Attack</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Warm Hole</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Spoofing</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Flooding</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Sink Hole</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Sybil</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

IV. CONCLUSION

This Survey aims to find the various security challenges and issues in wireless sensor networks. The reason why there is a need of security in WSNs, so that one can design the security protocol by focusing on the specific application of WSNs. The survey also focus on the constraints and limitation in WSNs that play a vital role in security issues and classified the different types of based on these limitations of WSNs.

REFERENCES


